
 <p>Arman Process Journal (APJ) Quarterly Journal of ICT APJ License Number: 87090</p>	<p>Arman Process Journal (APJ) Homepage: https://www.armanprocessjournal.ir</p>	
---	---	---

A Decentralized Exchange System Development based on the Blockchain Technology

Zahra Ghaemmaghami¹, Davood Mohammadpour^{2*}

¹ Department of Computer Engineering, Faculty of Management and Accounting, Qazvin Branch, Islamic Azad University, Qazvin, Iran

² Department of Computer Engineering, Faculty of Management and Accounting, Qazvin Branch, Islamic Azad University, Qazvin, Iran

ABSTRACT

RESEARCH PAPER

Received: 10 July 2024

Accepted: 14 November 2024

KEYWORDS:

*Blockchain,
Decentralized Exchange,
Digital Currency,
Platform,*

¹ **Corresponding author:**

✉ d.mohammadpour@iau.ac.ir

Nowadays, blockchains are best known for their vital role in digital currency systems in maintaining a secure and decentralized record of transactions, but their use cases are not limited to digital currencies. Blockchains can be used to make data immutable in any industry. A decentralized cryptocurrency exchange is a new type of cryptocurrency market trading platform that eliminates all intermediaries, enables digital market trading, and uses blockchain technology and smart contracts, and is very secure. Due to the necessity and importance of the increasing development of blockchain-based decentralized digital exchanges, this article first introduces the achievements and benefits of these exchanges and then, based on a case study, a basic application system is developed to create a decentralized exchange for buying and selling tokens using smart contracts. Using blockchain technology, this system enables the secure and transparent exchange of VoteCoin tokens. Its user interface, using React and interacting with MetaMask, allows users to easily interact with the system and participate in the buying and selling of tokens. This approach provides a foundation for a practical and tangible understanding of decentralized digital exchanges and their functioning, and can serve as a guide for developers and users in this field.

نشریه تخصصی آرمان پردازش، دوره ۵، شماره ۴، زمستان ۱۴۰۳



فصلنامه تخصصی آرمان پردازش
(APJ)

Homepage: www.armanprocessjournal.ir



رویکرد توسعه سیستم صرافی غیرمتمرکز براساس تکنولوژی بلاکچین

زهرا قائم مقامی^۱، داوود محمدپور^{۲*}

گروه مهندسی کامپیوتر، دانشکده مدیریت و حسابداری، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران
گروه مهندسی کامپیوتر، دانشکده مدیریت و حسابداری، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران

چکیده

امروزه بلاکچین بیشتر به دلیل نقش حیاتی در سیستم‌های ارزش‌های دیجیتال برای حفظ یک رکورد امن و غیرمتمرکز در تراکنش‌ها شناخته می‌شوند، اما موارد استفاده از آن‌ها به ارزش‌های دیجیتال محدود نمی‌شود. بلاک چین را می‌توان برای تغییرناپذیر کردن داده‌ها در هر صنعتی مورد استفاده قرار داد. صرافی ارز دیجیتال غیر متمرکز نوع جدیدی از پلتفرم‌های معاملاتی بازار ارز دیجیتال می‌باشد که با حذف تمامی واسطه‌ها، امکان معامله بازارهای دیجیتال را فراهم نموده و از تکنولوژی بلاکچین و قراردادهای هوشمند استفاده می‌نماید و بسیار ایمن است. به دلیل ضرورت و اهمیت توسعه روزافزون صرافی‌های غیرمتمرکز دیجیتال برپایه بلاکچین در این مقاله ابتدا به معرفی دستاوردها و مزایای این صرافی‌ها پرداخته و سپس براساس مطالعه موردی یک سیستم کاربردی پایه برای ایجاد یک صرافی غیرمتمرکز برای خرید و فروش توکن‌ها با استفاده از قراردادهای هوشمند توسعه می‌یابد. با استفاده از فناوری بلاک‌چین، این سیستم امکان تبادل امن و شفاف توکن‌های VoteCoin را فراهم می‌نماید. رابط کاربری آن با استفاده از React و تعامل با MetaMask به کاربران این امکان را می‌دهد که به راحتی با سیستم ارتباط برقرار کنند و در خرید و فروش توکن‌ها شرکت کنند. این رویکرد بنیانی برای درک کاربردی و ملموس صرافی‌های غیرمتمرکز دیجیتال و عملکرد آنها فراهم نموده و می‌تواند به عنوان راهنمایی برای توسعه‌دهندگان و کاربران این حوزه باشد.

مقاله پژوهشی

تاریخ دریافت مقاله: ۱۴۰۳/۴/۲

تاریخ پذیرش: ۱۴۰۳/۸/۲۵

واژگان کلیدی:

بلاکچین،

صرافی غیرمتمرکز،

ارزدیجیتال،

پلتفرم،

مقدمه

موجود در تمامی گره‌ها تغییر کند. علاوه بر این ساختار بلاکچین نیز به گونه‌ای است که تغییر اطلاعات یک بلاک باعث نامعتبر شدن آن خواهد شد [۳].

صرافی ارز دیجیتال غیر متمرکز^۲ نوع جدیدی از پلتفرم‌های معاملاتی بازار ارز دیجیتال میباشد که با حذف تمامی واسطه‌ها و با اتصال کیف پول، امکان معامله در این بازار را برای شما فراهم میکند. این نوع صرافی‌ها که از تکنولوژی بلاکچین و قرارداد هوشمند استفاده میکنند دارای ارز دیجیتال کاربران را نزد خود نگهداری نمیکنند و از این نظر بالاترین امنیت ممکن را دارند و از خطر هک و سرقت دارایی توسط صرافی در امان میباشند [۴]. رشد سریع استفاده از صرافی‌های غیرمتمرکز، بیانگر وجود مزایایی است که از نظر برخی کاربران بازار کریپتوکارنسی، در الویت قرار دارند. در ادامه به برخی از این مزایا اشاره می‌کنیم [۵-۷]:

- امنیت: صرافی‌های غیرمتمرکز، برای اتصال به کیف پول‌ها و انجام تراکنش‌ها احتیاجی به کلیدهای خصوصی شما ندارند. در صرافی‌های غیر متمرکز، امکان خرید و فروش ارزهای دیجیتالی بیشتری فراهم است و این صرافی‌ها در مقابل حملات سایبری امنیت بیشتری دارند.
- حضانت: یکی از کلیدی‌ترین مزیت‌های صرافی غیرمتمرکز، حضانت از اطلاعات هویتی و همچنین محافظت از کلیدهای خصوصی کاربران است. اساساً صرافی‌های غیرمتمرکز برای اتصال و انجام تراکنش‌ها احتیاجی به کلیدهای خصوصی ندارند.
- تنوع: در صرافی‌های متمرکز، فقط ارزهای دیجیتالی امکان فعالیت دارند که مانعی از لحاظ قانونی و مالیاتی برای خرید و فروش آن‌ها وجود نداشته باشد، اما می‌دانیم که به دلیل عدم وجود سقف برای افزایش قیمت یک ارز مجازی به صورت روزانه، با استفاده از صرافی متمرکز، بخش بزرگی از بازار را از دست خواهیم داد. اما در صرافی‌های غیر متمرکز، امکان خرید و فروش این ارزها فراهم است که خود عاملی در محبوبیت این نوع از صرافی‌ها است [۸-۹].

در سال‌های اخیر تکنولوژی ارزهای دیجیتال در حوزه اقتصاد دیجیتال و تجارت الکترونیک بسیار مورد توجه قرار گرفته است. از آنجایی که این فناوری اساس کار ارزهای دیجیتال است، اهمیت زیادی دارد که فرایند کارکرد بلاکچین در صنعت خدمات مرتبط بررسی و واکاوی شود. بلاک چین^۱ شبکه‌ای است که با استفاده از تکنولوژی‌های غیرمتمرکز و رمزنگاری، تاریخچه تمام تراکنش‌های انجام شده با دارایی‌های دیجیتال را در یک دفتر کل دیجیتال و عمومی ذخیره می‌کند. امکان تغییر در اطلاعات ذخیره شده در بلاک چین وجود ندارد و تمام اطلاعات ثبت شده در آن به صورت شفاف در اختیار کاربران قرار می‌گیرد. در واقع شبکه بلاکچین همان چیزی است که حذف بانک‌ها و مؤسسات اقتصادی و مالی از تراکنش‌های دارایی‌های دیجیتال را امکان‌پذیر کرده و امنیت ارزهای دیجیتال را تضمین می‌کند؛ موضوعی که باعث شده اخیراً دارایی‌های دیجیتال کاربران و طرفداران زیادی پیدا کنند [۱].

بلاک چین‌ها بیشتر به دلیل نقش حیاتی در سیستم‌های ارزهای دیجیتال برای حفظ یک رکورد امن و غیرمتمرکز در تراکنش‌ها شناخته می‌شوند، اما موارد استفاده از آن‌ها به ارزهای دیجیتال محدود نمی‌شود. بلاک چین‌ها را می‌توان برای تغییرناپذیر کردن داده‌ها در هر صنعتی مورد استفاده قرار داد. از آن‌ها می‌توان برای ایجاد سیستم‌های مدیریت زنجیره تأمین، سیستم‌های رای‌گیری و موارد دیگر استفاده کرد. فناوری بلاک چین این پتانسیل را دارد که صنایع مختلف را با ایجاد اعتماد، امنیت و کارایی متحول کند [۲]. در واقع می‌توان گفت بلاکچین یک دفتر کل دیجیتال بزرگ است که اطلاعات تراکنش‌های شبکه به شکل دقیقی در آن ذخیره می‌شود. هر اطلاعاتی برای اینکه وارد شبکه شود باید توسط یک امضای دیجیتال تأیید شود و مورد تأیید سایر اعضای شبکه نیز قرار بگیرد. هیچکس مالک یک شبکه بلاک چین نیست و همه افراد می‌توانند به تمامی اطلاعات ثبت شده در شبکه دسترسی داشته باشند؛ اما نمی‌توانند در اطلاعات تغییری ایجاد کنند. زیرا تمام اطلاعات شبکه در هر گره ذخیره می‌شود و برای تغییر آن باید کل نسخه‌های کپی

² Decentralized Exchanges (DEX)

¹ Blockchain

خواهد بود که حتی یک لوگوی معتبر برای نمایش آن‌ها نیز ساخته نشده، این موضوع بسیار خطرناک است زیرا افراد سودجو می‌توانند با تشویق آماتورهای بازار به خرید توکن‌های ساختگی، کلاهبرداری‌های بزرگی را رقم بزنند که در این صورت قربانی‌های کلاهبرداری قادر به فروش توکن‌ها نخواهند بود [۱۵].

بنابراین مطالب عنوان شده صرافی‌های غیرمتمرکز نوعی از صرافی‌های ارز دیجیتال هستند که امکان تراکنش‌های مستقیم نقطه به نقطه را در یک پلتفرم امن بدون نیاز به واسطه، فراهم می‌کنند. صرافی غیرمتمرکز از تکنولوژی بلاکچین، قرارداد هوشمند و معاملات نقطه به نقطه بهره می‌گیرد تا امکان بیشتری برای کنترل، حریم خصوصی، ناشناس بودن، شفافیت و امنیت بر روی دارایی کاربران حین انجام معاملات فراهم کند. با بهره‌گیری از این فناوری‌ها، صرافی‌های غیرمتمرکز امکان کنترل کامل کاربران بر دارایی‌هایشان، حفظ حریم خصوصی و انجام تراکنش‌های شفاف و امن را فراهم می‌آورند. در این مقاله قصد داریم الزامات و بستر مورد نیاز جهت توسعه صرافی‌های غیرمتمرکز را بررسی و معرفی نمائیم.

انواع پلتفرم‌های صرافی غیرمتمرکز

در غیاب یک مرجع مرکزی، صرافی‌های غیرمتمرکز از سرورهای توزیعی استفاده می‌کنند که تحت شرایط تعیین شده خاص خود اجرا می‌شوند و هر معامله را در مخزن آنلاین ثبت می‌کنند. این معاملات مطمئن، نمایانگر بخشی از بازار دارایی‌های دیجیتالی است که عمدتاً بخش کوچک‌تری نسبت به بازار متمرکز است. بورس‌های سنتی سهام خریداران و فروشندگان را در یک مکان ادغام می‌کند، اطمینان حاصل می‌کند که معامله‌گران می‌توانند با تأمین نقدینگی، در موقعیت‌های لازم با سهولت به بازار وارد شوند. در صرافی‌های غیرمتمرکز، امکان خرید و فروش ارزهای دیجیتالی بیشتری فراهم است و این صرافی‌ها در مقابل حملات سایبری امنیت بیشتری دارند. اساساً طراحی پلتفرم صرافی ارز دیجیتال به طور کلی به سه نوع تقسیم می‌شود که از قرار زیر است [۱۹-۱۶]:

- معاملات قابل اعتماد: در صرافی‌های غیرمتمرکز، مبادلات تجاری از طریق قراردادهای هوشمند تجاری انجام می‌پذیرد و همین دلیل کافی است تا مبادلات تحت صرافی غیرمتمرکز، کمتر مورد حمله هکرها قرار بگیرد.
- کارمزد پایین: در صرافی‌های غیرمتمرکز میزان کارمزد دریافتی صرافی با توجه به میزان کاربرانی که در حال معامله هستند تغییر می‌کند، اما به مراتب پایین‌تر از میزان کارمزد در صرافی‌های متمرکز است.
- درکنار همه دستاوردها و مزایای ذکر شده صرافی‌های غیرمتمرکز دارای معایبی نیز می‌باشند. مهمترین معایب در این حوزه به شرح زیر می‌باشد [۱۰-۱۳]:
- نداشتن قابلیت بازبایی: همان‌طور که پیش‌تر اشاره شد، اساساً هیچ نهاد متمرکزی برای نظارت بر فرآیندهای یک صرافی غیرمتمرکز وجود ندارد. به زبان ساده‌تر، اگر کلیدهای خصوصی مفقود شود یا یک تراکنش اشتباه انجام بشود، هیچ تیم پشتیبانی وجود ندارد که به مشکل رسیدگی کند و تراکنش‌ها صرفاً بر اساس قراردادهای هوشمند تنظیم و اجرا می‌شوند [۱۴ و ۱۱].
- نقدینگی پایین: موضوعی که می‌تواند ارزش و کارکرد یک صرافی را بیش از پیش بالا ببرد، بالا بودن نقدینگی آن صرافی است، اما در صرافی‌های غیرمتمرکز شاهد نقدینگی کمتری هستیم، این یعنی در طرف دیگر یک معامله افراد کمتری وجود خواهند داشت که این موضوع یکی از معایب بزرگ صرافی‌های غیرمتمرکز است.
- سرعت پایین: معاملات در صرافی‌های غیرمتمرکز نیاز به بازه زمانی بیشتری برای تایید شدن دارند. دلیل اصلی این موضوع پایین بودن میزان نقدینگی صرافی‌های غیرمتمرکز و تعداد کم کاربران این صرافی‌ها است.
- لیست شدن توکن‌های نامعتبر: زمانی که یک کاربر در لیست یک صرافی غیرمتمرکز جست و جو کند، بدون شک شاهد تعداد زیادی از توکن‌ها

صرافی‌های غیرمتمرکز به عنوان بازیگران اصلی در دنیای ارزهای دیجیتال، آینده‌ای بسیار روشن پیش رو دارند. با پیشرفت فناوری بلاکچین و افزایش پذیرش ارزهای دیجیتال، انتظار می‌رود که DEX ها به تدریج با صرافی‌های متمرکز رقابت زیادی داشته باشند. همانطور که در بخش قبل بیان شد، دلایل این امر امنیت، سرعت، دقت و شفافیت بالاتر تراکنش‌های مالی می‌باشد. در بخش بعد مطالعه موردی جهت توسعه سیستم صرافی غیرمتمرکز در بلاکچین را ارائه خواهیم نمود.

مطالعه موردی

مطالعه موردی در این پروژه شامل دو قرارداد هوشمند به نام‌های VCTExchange و VoteCoin است که هدف آن‌ها ایجاد یک بازار غیرمتمرکز برای خرید و فروش توکن‌های VCT (VoteCoin) است. کاربران می‌توانند توکن‌های VCT را با استفاده از اتریوم خریداری یا به فروش برسانند و از مزایای این سیستم بهره‌برداری کنند. این پروژه با استفاده از فناوری بلاک‌چین و قراردادهای هوشمند نوشته شده است و ارتباط آن با یک اپلیکیشن مبتنی بر React فراهم شده است. شکل زیر نمای کلی از داشبرد پروژه را نمایش می‌دهد:

- AMM: یکی از انواع طراحی صرافی غیرمتمرکز AMM است. در این نوع از صرافی‌ها برخلاف صرافی‌های معمول به جای سیستم سفارش‌گیری به پروتکل‌ها متکی هستند. AMM ها بر اساس اصول استخرهای نقدینگی کار می‌کنند. یعنی به جای تطبیق مستقیم خریدار و فروشنده، از نقدینگی ارائه شده توسط کاربران برای تسهیل تریدها استفاده می‌کنند
- Order Book DEX: طراحی سایت صرافی DEX به صورت Order Book به این صورت است که تطبیق معاملات و سفارش‌گذاری‌ها توسط یک موتور تطبیق مشابه صرافی‌های متمرکز و سنتی عمل می‌کند. یعنی از Order Book برای مطابقت سفارش‌های خرید و فروش تکیه می‌کنند.
- DEX Aggregator: در واقع یک پروتکل مالی است که دسترسی سرمایه‌گذاران و تریدرها را به انواع استخرهای نقدینگی و معاملاتی در یک داشبورد تسهیل می‌کند. یعنی این پلتفرم‌های نقدینگی را از چندین DEX ترکیب می‌کند تا به کاربران دسترسی بهتری به جفت ارزهای معاملاتی و دریافت قیمت بهتر ارائه بدهد.

The screenshot shows a web interface for VCTExchange. At the top, there are navigation buttons: 'Set Vote Coin', 'Withdraw Benefit | Benefit: 0 ETH', 'Buy', 'Sell', and 'Request Token'. A status bar indicates 'Connected: 0xB575...60aC | Balance: 50 VCT'. Below this, there are two tables: 'SellOrders' and 'BuyOrders'.

Order ID	Price (ETH)	Amount (VCT)
0x87ed87bac7887d15bfa1b2d6a0d313b672ee6f3a4081022f850cae37c090a16	3	30
0x518e6eb3094d8bbf74b7ac491ba38ebb425736eaebcf5ec89d9168416f2ce	4	20

Order ID	Price (ETH)	Amount (VCT)
0xB313fabf159c8a1b06b3ae1af66df670b3c91fb4aff576a33f4a0666566e82	2	1

تصویر ۱. نمای کلی از داشبرد پروژه توسعه یافته

اجزای توسعه یافته پروژه به شرح زیر می‌باشند:

- `balanceOf`: موجودی توکن‌های یک کاربر برای سال جاری را نمایش می‌دهد.
- `addParticipateYear`: سال‌هایی که کاربر در آن‌ها توکن دریافت کرده را ذخیره می‌کند.

مثال: در این قرارداد، اگر کاربری قصد انتقال توکن‌ها به کاربر دیگری داشته باشد، می‌تواند از تابع `transfer` استفاده کند که موجودی سال جاری کاربر را بررسی کرده و در صورت کافی بودن موجودی، توکن‌ها را منتقل می‌کند.

۲. قرارداد `VCTExchange`: قرارداد `VCTExchange` به عنوان یک بازار برای تبادل توکن‌ها عمل می‌کند. کاربران می‌توانند سفارشات خرید و فروش خود را در این قرارداد ثبت کنند و سیستم به صورت خودکار بهترین سفارشات را برای انجام تراکنش‌ها تطبیق می‌دهد.

• ویژگی‌ها و توابع:

- `buyTokenByETH`: این تابع به کاربران این امکان را می‌دهد که با ارسال اتریوم، توکن‌های `VCT` خریداری کنند.
- `sellTokenToETH`: کاربران می‌توانند توکن‌های `VCT` خود را به فروش برسانند و در ازای آن ارز دیجیتال اتریوم دریافت کنند.

○ `tryMatchOrders`: این تابع اساساً برای تطبیق سفارشات خرید و فروش استفاده می‌شود.

○ `withdrawBenefit`: مالک قرارداد می‌تواند مزایای حاصل از تفاوت قیمت خرید و فروش توکن‌ها را برداشت کند.

○ `setVoteCoin`: این تابع برای تنظیم آدرس قرارداد `VoteCoin` استفاده می‌شود.

مثال: اگر کاربری یک سفارش خرید توکن ثبت کند و کاربر دیگری یک سفارش فروش ثبت کرده باشد که قیمت آن به هم نزدیک است، این تابع سفارشات را تطبیق داده و تراکنش‌ها را انجام می‌دهد.

• `VoteCoin Contract` (توکن `VCT`): این قرارداد، توکن `ERC20` استاندارد است که به کاربران امکان دریافت و انتقال توکن‌های `VCT` را می‌دهد. هر سال به هر کاربر یک مقدار معین توکن تعلق می‌گیرد. این توکن‌ها برای مشارکت در خرید و فروش در `VCTExchange` استفاده می‌شوند.

• `VCTExchange Contract`: این قرارداد هوشمند به عنوان یک بازار برای خرید و فروش توکن‌های `VCT` عمل می‌کند. کاربران می‌توانند سفارشات خرید یا فروش خود را در این قرارداد ثبت کنند و پس از آن، سیستم به صورت خودکار سفارشات خرید و فروش را با یکدیگر تطبیق می‌دهد. این سیستم از قابلیت‌هایی همچون ذخیره سفارشات، تطبیق سفارشات، و واریز مزایا به مالکان استفاده می‌کند.

• `Frontend` (واسط کاربری): واسط کاربری این پروژه با استفاده از `React` نوشته شده است و کاربران از طریق این واسط می‌توانند به قراردادهای هوشمند متصل شوند. همچنین، امکان مشاهده موجودی توکن‌ها، ارسال سفارشات خرید و فروش، درخواست توکن برای سال جاری و برداشت مزایا از سیستم وجود دارد.

همچنین جزئیات قراردادهای هوشمند به شرح زیر می‌باشد:

۱. قرارداد `VoteCoin`: `VoteCoin` یک توکن `ERC20` است که به هر کاربر، بر اساس سال، مقدار مشخصی از توکن‌ها اهدا می‌شود. این قرارداد از تابع `requestTokenForThisYear` برای درخواست توکن‌ها استفاده می‌کند و همچنین از توابع انتقال برای جابجایی توکن‌ها بین کاربران بهره می‌برد.

• ویژگی‌ها و توابع:

○ `requestTokenForThisYear`: هر کاربر سیستمی تنها یک بار در سال توکن دریافت می‌کند.

○ `transfer`: برای انتقال توکن‌ها بین کاربران استفاده می‌شود.

متصل شود. پس از اتصال، اطلاعات حساب کاربری و موجودی کاربر بارگذاری می‌شود.

۲. ارسال سفارش خرید یا فروش: زمانی که کاربر یک سفارش خرید یا فروش ثبت می‌کند، بخش فرانت‌اند با استفاده از متدهای `sendBuyOrder` و `sendSellOrder` سفارشات را به قرارداد `VCTExchange` ارسال می‌کند. این اطلاعات شامل قیمت و مقدار توکن‌ها است.

۳. نمایش سفارشات: پس از ثبت سفارش، فرانت‌اند اطلاعات موجود در قرارداد `VCTExchange` را از طریق متدهایی مانند `loadBuyOrders` و `loadSellOrders` بارگذار می‌کند و به کاربر نمایش می‌دهد.

۴. درخواست توکن برای سال جاری: از آنجا که هر کاربر تنها یک بار در سال می‌تواند توکن دریافت کند، با استفاده از متد `requestTokenForThisYear` کاربر می‌تواند توکن‌های `VCT` برای سال جاری درخواست کند. در پایان لازم به ذکر است، این پروژه از قابلیت‌های امنیتی مانند استفاده از تابع `onlyOwner` در قرارداد `VCTExchange` برای محدود کردن برخی عملکردها به مالک قرارداد استفاده می‌کند. همچنین این سیستم می‌تواند برای استفاده در بازارهای مشابه یا افزودن ویژگی‌های جدید مانند ایجاد توکن‌های مختلف یا بهبود الگوریتم‌های تطبیق سفارش گسترش یابد.

نتیجه‌گیری

این پروژه یک سیستم پایه برای ایجاد یک بازار غیرمتمرکز برای خرید و فروش توکن‌ها با استفاده از قراردادهای هوشمند است. با استفاده از فناوری بلاک‌چین، این سیستم امکان تبادل امن و شفاف توکن‌های `(VCT)` را فراهم می‌کند. رابط کاربری آن با استفاده از `React` و تعامل با `MetaMask` به کاربران این امکان را می‌دهد که به راحتی با سیستم ارتباط برقرار کنند و در خرید و فروش توکن‌ها شرکت کنند. این مستندات پایه‌ای برای درک کلی پروژه و

نهایتاً در بخش فرانت‌اند، از کتابخانه `React` برای ساخت واسط کاربری استفاده شده است. کاربران از این طریق می‌توانند به راحتی با قراردادهای هوشمند تعامل کنند. اپلیکیشن به کاربران این امکان را می‌دهد که:

- به `MetaMask` متصل شوند و حساب کاربری خود را انتخاب کنند.
- موجودی توکن‌های `VCT` خود را مشاهده کنند.
- سفارشات خرید و فروش توکن ثبت کنند.
- توکن‌های `VoteCoin` برای سال جاری درخواست کنند.
- مزایای حاصل از خرید و فروش را برداشت کنند.

توضیح ساختار کد: `React`

- `useState`: از `useState` برای ذخیره مقادیر مختلف مثل حساب کاربری، موجودی، سفارشات خرید و فروش، و وضعیت مدیریت استفاده شده است.
- `useEffect`: از `useEffect` برای بارگذاری داده‌های مختلف مثل قراردادهای هوشمند، موجودی و سفارشات استفاده می‌شود.
- توابع اصلی:

- `connectToMetaMask`: برای اتصال به `MetaMask` و بارگذاری اطلاعات حساب کاربری.

- `sendSellOrder` و `sendBuyOrder`

برای ارسال سفارشات خرید و فروش.

- `loadBenefit` و `loadBalance`: برای بارگذاری موجودی و مزایای قراردادهای هوشمند.

- `addWalletListener`: برای گوش دادن به تغییرات حساب کاربری در `MetaMask`.

نحوه تعامل قراردادهای هوشمند با بخش فرانت‌اند بصورت و به شرح زیر می‌باشد:

۱. اتصال به `MetaMask`: کاربر پس از بارگذاری

صفحه، می‌تواند از طریق

متد `connectToMetaMask` به `MetaMask`

oversight. Benefits, and Oversight (June 15, 2024). 2024 Jun 15.

[10] Ciesielska-Maciągowska D, Spyra Ł. Cryptocurrency exchanges in the decentralized finance system. *Kwartalnik Nauk o Przedsiębiorstwie*. 2025 Mar 31;75(1):23-33.

[11] Johnson KN. Decentralized finance: Regulating cryptocurrency exchanges. *Wm. & Mary L. Rev.* 2020;62:1911.

[12] Heimbach L, Wang Y, Wattenhofer R. Behavior of liquidity providers in decentralized exchanges. *arXiv preprint arXiv:2105.13822*. 2021 May 28.

[13] Nummelin S. Risks and benefits of centralized and decentralized cryptocurrency exchanges and services.

[14] Dai C. DEX: A DApp for the decentralized marketplace. *Blockchain and Crypt Currency*. 2020 Apr 16;95.

[15] Mohan V. Automated market makers and decentralized exchanges: a DeFi primer. *Financial Innovation*. 2022 Feb 14;8(1):20.

[16] Schär F. Decentralized finance: on blockchain and smart contract-based financial markets. *Review of the Federal Reserve Bank of St Louis*. 2021;103(2):153-74.

[17] Röckener M. *Centralized Crypto Exchanges Incorporating Decentralized Features: Factors Driving Implementation and Impact on the Competitive Landscape* (Doctoral dissertation, Hochschule Mittweida).

[18] Lehar A, Parlour C. Decentralized exchange: The uniswap automated market maker. *The Journal of Finance*. 2025 Feb;80(1):321-74.

[19] Helmy B, Cachin C, Micic J. Exploring blockchain-based decentralized exchanges [Internet]. 2021 Oct 10

عملکرد آن فراهم می‌کند و می‌تواند به عنوان راهنمایی برای توسعه‌دهندگان و کاربران باشد.

مراجع

[1] Capponi A, Jia R. The adoption of blockchain-based decentralized exchanges. *arXiv preprint arXiv:2103.08842*. 2021 Mar 16.

[2] Wu X, Deng W, Quan Y, Zhang L. Trust dynamics and market behavior in cryptocurrency: A comparative study of centralized and decentralized exchanges. *arXiv preprint arXiv:2404.17227*. 2024 Apr 26.

[3] Han J, Huang S, Zhong Z. Trust in defi: an empirical study of the decentralized exchange. Available at SSRN. 2021 Jul 26;3896461.

[4] Patel H. A pure block chain based decentralized exchange. *Cryptology ePrint Archive*. 2014.

[5] Aspris A, Foley S, Svec J, Wang L. Decentralized exchanges: The “wild west” of cryptocurrency trading. *International Review of Financial Analysis*. 2021 Oct 1;77:101845.

[6] Hägele S. Centralized exchanges vs. decentralized exchanges in cryptocurrency markets: A systematic literature review. *Electronic Markets*. 2024 Dec;34(1):33.

[7] Lin LX. Deconstructing decentralized exchanges. *Stan. J. Blockchain L. & Pol'y*. 2019;2:58.

[8] Warren W, Bandeau A. Ox: An open protocol for decentralized exchange on the Ethereum blockchain. URL: <https://github.com/OxProject/whitepaper>. 2017 Feb 21:04-18.

[9] Harvey CR, Hasbrouck J, Saleh F. The evolution of decentralized exchange: Risks, benefits, and

COPYRIGHTS

©2024 by the authors. Published by the **Islamic Azad University, Khodabandeh Branch, Zanjan**. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY 4.0)

